DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Review of DHS Component Plans of Action and Milestones for Financial System Security

OIG-08-63

June 2008

Office of Inspector General

U.S. Department of
Homeland Security
Washington, DC 20528

Homeland
Security

June 4, 2008

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report summaries the results of KPMG observations and provides the CIO and CFO with recommendations based on best practices to help enhance the existing POA&M process at the DHS components. The independent accounting firm KPMG LLP (KPMG) performed the review of the DHS POA&Ms in an effort to support DHS' compliance with the Department of Homeland Security Financial Accountability Act of 2004 (DHS FAA), which requires DHS to obtain an ICOFR audit opinion. KPMG is responsible for the attached report dated May 13, 2008 and the conclusions expressed in it.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report

Richard L. Skinner

Richard L. Skinner
Inspector General

KPMG LLP
2001 M Street, NW
Washington, DC 20036

May 13, 2008

Inspector General
U.S. Department of Homeland Security

Chief Financial Officer
U.S. Department of Homeland Security

Chief Information Officer
U.S. Department of Homeland Security

KPMG LLP (KPMG) assessed the status of the Information Technology (IT) Plans of Action and Milestones (POA&M) implemented by the United States Coast Guard (USCG), Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and Federal Emergency Management Agency (FEMA) that relate to the financial systems security material weakness cited in the Independent Auditors' Report included in the Department's Fiscal Year (FY) 2006 *Performance and Accountability Report.* In accordance with our contract, GS-23F-8127H, Task Order, TPD-FIG-05-K-00045, this performance audit had the following four objectives:

1) Are the POA&Ms well-written, to include milestones and specific, actionable steps to correct the Department of Homeland Security's (DHS) material weakness in internal control related to financial IT systems?
2) Are the POA&Ms updated with milestones and continued steady progress?
3) Are the POA&Ms consistent with DHS' planned financial system consolidation?
4) Is there linkage between the IT POA&Ms and the Office of Management and Budget (OMB) Circular A-123 guidance issued by the DHS Chief Financial Officer (CFO)?

This performance audit is the first in a series of performance audits the Office of Inspector General (OIG) has engaged us to perform. We conducted test work over the period of November 15 through December 12, 2007 in accordance with *Generally Accepted Government Auditing Standards (GAGAS)* issued by the Comptroller General of the United States. Our testing consisted of inquiries of DHS management and personnel and inspection of relevant documentation. This report summarizes the results of our observations and provides the DHS Office of the Inspector General (OIG), Chief Information Officer (CIO) and CFO with recommendations based on best practices to help enhance the existing POA&M process at the DHS component agencies.

Since the conclusion of fieldwork on December 12, 2007, we have not performed any additional procedures with respect to these objectives of the performance audit and have no obligation to update this report or to revise the information contained herein to reflect events occurring subsequent to our conclusion of fieldwork.

KPMG understands that it is the OIG's responsibility to distribute this final report. We have authorized the OIG to send this report electronically to DHS for the convenience of the Department. However, only the final hard copy of our report should be deemed our final work product.

Very truly yours,

KPMG LLP

Table of Contents

Executive Summary

The Department of Homeland Security (DHS) Office of Inspector General (OIG) engaged KPMG LLP (KPMG) to assist the OIG in assessing the status of the Information Technology (IT) Plans of Action and Milestones (POA&M) implemented by the United States Coast Guard (USCG), Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and Federal Emergency Management Agency (FEMA) that relate to the financial systems security material weakness cited in the Independent Auditors' Report included in the Department's Fiscal Year (FY) 2006 *Performance and Accountability Report.* The performance audit had the following four objectives:

1) Are the POA&Ms well-written, to include milestones and specific, actionable steps to correct the Department of Homeland Security's (DHS) material weakness in internal control related to financial IT systems?
2) Are the POA&Ms updated with milestones and continued steady progress?
3) Are the POA&Ms consistent with DHS' planned financial system consolidation?
4) Is there linkage between the IT POA&Ms and the Office of Management and Budget (OMB) Circular A-123 guidance issued by the DHS Chief Financial Officer (CFO)?

We evaluated the POA&M process and status of IT POA&Ms through review of the IT POA&Ms and discussion with the in-scope component, DHS Office of Chief Information Officer (OCIO), and DHS Office of Chief Financial Officer (OCFO) personnel. This report is intended to provide the in-scope DHS components, the OIG, the OCIO, and the OCFO with information on the best practices and weaknesses of the current POA&M process employed by the agency, as well as recommendations for enhancing the existing process.

This audit was performed in accordance with *Generally Accepted Government Auditing Standards (GAGAS),* issued by the Comptroller General of the United States, specifically, the standards for performance audits.

Results and Recommendations

Objective 1: Are the POA&Ms well-written, to include milestones and specific, actionable steps to correct the DHS' material weakness in internal control related to financial IT systems?

POA&M milestones are not written to represent unique, actionable steps. Milestones are often copied from the recommendation section of the FY 2006 Notice of Finding and Recommendation (NFR) issued to the component. Similarly, the majority of milestones are written to address the condition of the weakness, rather than the underlying root cause of the weakness. Finally, milestones are not developed with sufficient detail to be used effectively in addressing the weakness. Many weaknesses have one milestone, no milestones, or are duplicated multiple times throughout the POA&M for the same weakness.

Recommendations

We recommend that FEMA, ICE, TSA, and USCG:

1) Conduct a formal root cause analysis for IT weaknesses in order to determine the appropriate corrective actions.
2) Review existing POA&M weaknesses and milestones to confirm that the root cause is being addressed.

3) Require the component Information System Security Manager (ISSM) to verify that the component is creating unique POA&M milestones to address the root cause of identified weaknesses, rather than using the NFR recommendations as milestones.
4) Require that the component ISSM ensure that POA&M milestones include reasonably scheduled completion dates.

Additionally, we recommend the OCIO to:

1) Update DHS 4300A, Attachment H, *POA&M Process Guide*, to include a requirement for quarterly milestone completion dates, and to prohibit components from only using NFR recommendations as milestones, unless the root cause analysis is in agreement with the NFR recommendation.
2) Enhance root cause analysis guidance and training provided to component personnel.

Objective 2: Are the POA&Ms updated with milestones and continued steady progress?

POA&M weaknesses and milestones are not consistently updated, or are updated with inaccurate status information. Weakness and milestone scheduled completion dates are not reasonable and do not include regular, timely tasks. As a result, the POA&Ms do not demonstrate continued steady progress in addressing IT weaknesses. Additionally, testing of the closure of POA&M weaknesses is not consistently performed to verify that weaknesses have been completely addressed.

Recommendations

We recommend that FEMA, TSA, and USCG create and implement an internal independent verification and validation (IV&V) process to verify and document the status of POA&M weaknesses. This process should include approvals for closure by the component ISSM and require the upload of artifacts into Trusted Agent FISMA (TAF) to support the closure of the NFRs.

Additionally, we recommend the OCIO to update DHS 4300A, Attachment H to require that components include testing and closure validation as a milestone for each POA&M weakness in order to verify that weaknesses are properly closed.

Objective 3: Are the POA&Ms consistent with DHS' planned financial system consolidation?

The DHS planned financial system consolidation effort is currently in the pre-implementation stage. We were unable to determine the impact of the consolidation effort on the component POA&Ms. As such, an accurate assessment could not be made as to whether POA&M milestones are consistent with the DHS system consolidation. No recommendations were made in relation to Objective 3.

Objective 4: Is there linkage between the IT POA&Ms and the OMB A-123 guidance issued by the DHS CFO?

The OCFO and OCIO have made progress in creating a strategy for resolving material weaknesses and building management assurances. However, there is currently a limited correlation between the POA&M process and the OCFO's OMB A-123 strategy. Additionally, the OCFO, OCIO, component CFOs, and CIOs need to better understand and integrate the role of IT general and application controls in the Internal Controls Over Financial Reporting (ICOFR) process. IT audit findings are primarily addressed by the component CIOs with little or no involvement from the OCFO, although such weaknesses also impact financial processes. If the OCIO, OCFO, and component CFO and CIO can work jointly to address IT weaknesses, management should be able to place increased reliance on the IT general controls environment and financial application controls and thus, improve the ICOFR process.

Recommendations

We recommend that the DHS OCFO and OCIO work together to jointly develop detailed standard operating procedures (SOP) for identifying and addressing each IT weakness and/or audit finding. These SOPs should include a recommended approach to address those findings in a collaborative effort from both the component CIO and CFO. This collaborative management approach should include a process to:

1) Delineate responsibility and ownership over remediation efforts;
2) Identify the necessary resources and funding sources; and
3) Plan to perform corrective action jointly, where appropriate.

Results and Recommendations

Objective 1: Are the Plans of Action and Milestones (POA&M) well-written, to include milestones and specific, actionable steps to correct the Department of Homeland Security's (DHS) material weakness in internal control related to financial Information Technology (IT) systems?

We conducted test work through inquiry of DHS Office of Chief Information Officer (OCIO), Transportation Security Administration (TSA), United States Coast Guard (USCG), Federal Emergency Management Agency (FEMA), and Immigration and Customs Enforcement (ICE) personnel, and inspection of DHS POA&M procedures and component POA&Ms in order to determine whether DHS component POA&Ms are well-written, and include milestones and specific, actionable steps. During the course of our test work, we made the following observations:

Milestones Are Not Written to Represent Unique, Actionable Steps

While we determined that the POA&Ms generally include all the key elements required by both the Office of Management and Budget (OMB) and the DHS 4300A, *Sensitive Systems Handbook*, Attachment H, *POA&M Process Guide*, we found that POA&M weaknesses and milestones are not written to represent effective actionable steps. Per the DHS POA&M guidance, DHS 4300A, Attachment H, milestones should not simply re-state the weakness description, but should rather describe an action needed to correct the weakness. In the four components' POA&Ms reviewed, milestones are often an exact copy of the recommendation from the Fiscal Year (FY) 2006 Notice of Finding and Recommendation (NFR) issued to the component. The recommendations issued during the Financial Statement Audit are general in nature and should be used as a starting point to determine the specific steps necessary to address the weakness identified. The milestones should effectively communicate the major steps that will be performed to correct a weakness.

Milestones Do Not Address the Root Cause of the Weakness

Milestones are written to address the conditions of the weaknesses, rather than the root cause. Correcting a condition does not necessarily address the underlying root cause of the condition. Additionally, without addressing the root cause, components are likely to find reoccurrences of the same weakness in the future. For example, at FEMA, a weakness detailed a number of configuration management weaknesses identified. FEMA's corrective actions only addressed the specific configuration management conditions, such as upgrading software, disabling unnecessary services, and updating non-compliant passwords. However, FEMA did not address the root cause or implement corrective action that would minimize future occurrences. A better approach would be for components to independently analyze the root cause of the weaknesses and develop milestones to address both the condition and the cause, using the audit recommendation as a baseline.

Milestones Do Not Include Sufficient Detail or Are Duplicated

For all of the four components' POA&Ms reviewed, we identified that milestones were not developed with sufficient detail to effectively address the weaknesses. Many weaknesses only have one associated milestone which does not sufficiently describe the steps necessary to completely address the weakness. Additionally, in FEMA's POA&M, we noted instances of weaknesses with no associated milestones. Detailed milestones are needed to ensure that all necessary steps are performed to resolve the root cause of the weakness. Furthermore, detailed milestones encourage a steady state of progress when remediating a weakness.

Duplicate weakness entries on the POA&M were also identified in TSA's and USCG's POA&Ms. We noted numerous cases in which one weakness or NFR appears multiple times. The use of duplicate entries for various weaknesses allows for the reporting of inaccurate data and status of weaknesses. Additionally, it may lead to concurrent updates within the POA&M for the same weakness in different fields. This may result in corrective actions not being traced back to the weakness.

Recommendations

We recommend that FEMA, ICA, TSA, and USCG:

1) Conduct a formal root cause analysis for IT weaknesses in order to determine the appropriate corrective action. The following would be the steps taken when performing a root cause analysis:

   - Identify and walk through the process associated with the weakness;
   - Perform an analysis to determine gaps within the process;
   - Find the root cause contributing to the gaps within the process;
   - Develop and implement identified solution; and
   - Observe the implementation of the solution to ensure effectiveness.

   Table 1, on the following page, documents an example POA&M which illustrates the level of detail recommended including milestones derived from root cause analysis.

2) Review existing POA&M weaknesses and milestones to confirm that the root cause is being addressed.

3) Require the component Information System Security Manager (ISSM) to verify that components are creating unique POA&M milestones to address the root cause of identified weaknesses, rather than using the NFR recommendations as milestones.

4) Require the component ISSM to ensure that POA&M milestones include reasonably scheduled completion dates. At a minimum, FEMA, ICE, TSA, and USCG should create milestones with quarterly completion dates. Table 1, on the following page, illustrates reasonably scheduled completion dates.

Additionally, we recommend that the OCIO:

1) Update DHS 4300A, Attachment H, to include the requirement for quarterly milestone completion dates, as well as to prohibit components from using NFR recommendations as milestones, unless the root cause analysis is in agreement with the NFR recommendations.

2) Enhance root cause analysis guidance and training provided to component personnel.

Table 1 – Example System-level Plan of Action and Milestones
Project ID, Project Name -- Department Homeland Security

Weakness	Point of Contact	Resources Required	Scheduled Completion Date	Milestones	Milestone Scheduled Completion Date	Changes to Milestones	Status
Excessive access for 15 terminated employees.	ISSO	$1,000	March 31, 2008	Remove the identified terminated user accounts.	December 31, 2007		Completed.
				Develop procedures for timely removal of terminated user accounts. This includes developing a new standard "delete user" form.	January 31, 2008		Ongoing.
				Develop and provide training to program managers and supervisors of new requirements.	February 29, 2008		Ongoing.
				Compare listing of terminated employees to the current system listing to verify there is no excessive access.	March 31, 2008		Ongoing.
Configuration management weaknesses and weak passwords identified.	ISSO	$2,000	May 30, 2008	Upgrade Oracle database to most current version.	November 15, 2007		Completed.
				Modify password configuration settings to comply with DHS standards.	November 15, 2007		Completed.
				Establish a program of quarterly vulnerability scans to identify new weaknesses.	March 31, 2008		Ongoing.
				Establish a patch management policy to identify and install patches and fixes on a monthly basis.	April 30, 2008		Ongoing.
				Run vulnerability scan to verify that previously identified configuration weaknesses are resolved.	May 31, 2008		Ongoing.

Objective 2: Are the POA&Ms updated with milestones and continued steady progress?

We conducted test work through inquiry of DHS OCIO, TSA, USCG, FEMA, and ICE personnel, and inspection of DHS POA&M procedures and component POA&Ms in order to determine whether DHS component POA&Ms are updated with milestones and continued steady progress. Through our test work, we identified that POA&M weaknesses and milestones are not consistently updated, or are updated with inaccurate status information. We made the following observations:

Scheduled Completion Dates Are Not Reasonable

We identified that "Scheduled Completion Dates" are not accurately derived or are not reasonable. At all four components, we found that the scheduled completion date for each milestone associated for a particular weakness was often the same as the overall weakness scheduled completion date, as illustrated in Table 2, below:

Weakness	Scheduled Completion Date	Milestone	Scheduled Completion Date
Configuration management weaknesses and weak passwords identified.	September 30, 2008	Upgrade Oracle database to most current version.	September 30, 2008
		Modify password configuration settings to comply with DHS standards.	September 30, 2008
		Establish a program of quarterly vulnerability scans to identify new weaknesses.	September 30, 2008
		Establish a patch management policy to identify and install patches and fixes on a monthly basis.	September 30, 2008
		Run vulnerability scan to verify that previously identified configuration weaknesses are resolved.	September 30, 2008

Table 2

Because the scheduled completion dates are several months in the future and do not include regular, timely tasks, no POA&M updates were required by component personnel until the milestones became overdue. As a result, the components may not update the milestone status on a quarterly basis as required by OMB and DHS 4300A, even though activities are occurring during the quarter to address the POA&M weakness. Additionally, without regularly scheduled milestones, the POA&Ms do not demonstrate continued steady progress in addressing IT weaknesses.

Testing of the Closure of POA&M Weaknesses Is Not Consistently Performed

At each of the four components, we noted that milestones are not appropriately documented to include requirements for the testing of the remedial action taken to verify that weaknesses have been completely addressed. DHS 4300A, Attachment H, suggests that corrective action testing should be incorporated into the weakness mitigation process and identified as a milestone. Testing the corrective action helps to ensure the weakness is effectively resolved.

Similarly, in the DHS 4300A, Attachment H, supervisory review by the component ISSM or individual system owner is not required when closing a POA&M weakness within Trusted Agent FISMA (TAF). There is no standard process or requirement for validating the closure of weaknesses. Specifically, Attachment H does not provide guidance on who should conduct testing of the remedial actions, testing standards, documentation requirements, or who should grant approval for closure of POA&M weaknesses. The DHS OCIO has suggested in the DHS 4300A, Attachment H that components should upload "artifacts" into TAF to support the closure of NFRs. Per Attachment H, the use of this feature is not required; however, we determined that the attachment is used inconsistently by the components. We found that ICE initiated an independent verification and validation (IV&V) process in order to verify and document the closure of POA&M weakness related to the FY 2006 financial statement audit NFRs. As a result of this IV&V process, ICE was able to successful close nearly all of the FY 2006 NFRs. However, ICE indicated that the IV&V process was not initiated until a status report of the FY 2006 NFRs was specifically requested by the DHS OCIO. Additionally, we noted that FEMA, TSA, and USCG have not implemented an IV&V process when closing POA&M weaknesses.

Without testing the corrective action and verifying closure of POA&M weaknesses, the POA&M may not be accurate and reflect the true security posture of the system and component environment. Additionally, we found that weaknesses associated with FY 2006 IT NFRs were often inappropriately designated as completed. Of the 121 NFRs examined in this performance audit, 31 NFRs were reported as closed by the components, but were reissued as part of the FY 2007 DHS financial statement audit.

Recommendations

We recommend that FEMA, TSA, and USCG create and implement an internal IV&V process to verify and document the status of POA&M weaknesses. This process should include approvals for closure by the component ISSM and require the upload of artifacts into TAF which would support closure.

Additionally, we recommend that the OCIO update DHS 4300A, Attachment H to require that components include testing and closure validation as a milestone for each POA&M weakness in order to verify that weaknesses are resolved.

Objective 3: Are the POA&Ms consistent with DHS' planned financial system consolidation?

We met with key personnel in the DHS Resource Management Transformation Office (RMTO) to discuss and gain an understanding of the planned DHS financial system consolidation. Additionally, we met with FEMA, ICE, TSA, and USCG personnel and reviewed the component POA&Ms to determine whether the POA&M milestones are consistent with the DHS plans for financial system consolidation.

The financial system consolidation is currently in the pre-implementation stage. RMTO has initiated an acquisition to identify a "Solutions Architect" to carry out the consolidation activities. Once the Solutions Architect has been identified, consolidation activities will commence. TSA's Oracle implementation will be deemed the baseline for the system consolidation beginning in June 2008. Beginning in FY 2009, smaller DHS components, such as the Office of Health Affairs, Departmental Operations, and Science and Technology will begin the migration process. ICE is tentatively scheduled to begin migration in FY 2010. Regarding USCG, FEMA, and the remaining DHS components, plans and timelines for migration to the TSA baseline have not been fully determined. These components will continue with their current financial system operations and plans for migration will be evaluated and determined in approximately three to four years.

Since the consolidation effort is currently in the pre-implementation stage, we were unable to determine the impact of the consolidation effort on the current TSA, USCG, FEMA, and ICE POA&Ms. As such, an accurate assessment could not be made as to whether POA&M milestones are consistent with the DHS system consolidation. No recommendations were made in relation to Objective 3.

Objective 4: Is there linkage between the IT POA&Ms and the Office of Management and Budget (OMB) Circular A-123 (A-123) guidance issued by the DHS CFO?

We met with OCFO, OCIO and component personnel and also reviewed relevant documentation to determine the linkage between the IT POA&Ms and the A-123 guidance issued by the DHS CFO.

The OCFO has developed the Internal Controls Over Financial Reporting (ICOFR) Playbook which outlines the OCFO's short and long term strategy and process to resolve material weaknesses and build the management assurance process. The ICOFR Playbook currently consists of two tracks. The first track focuses on developing Corrective Action Plans (CAP) to address financial process material weakness conditions. The second track focuses on building support for the Department's ICOFR assurance statement through management performed testing on areas without material weakness conditions.

Additionally, DHS plans to develop a third and fourth track for the ICOFR Playbook related to maintaining efficient, effective, and secure financial systems and internal controls over operations. This third track will focus on becoming compliant with the objectives of the Federal Financial Management Improvement Act (FFMIA), including federal financial management system requirements, applicable federal accounting standards, and the United States Standard General Ledger (USSGL). Additionally, these tracks will describe the relationship between the IT systems consolidation and internal controls.

The OCIO has developed DHS 4300A, Attachment R, *Compliance Framework for CFO Designated Financial Systems*. This document details the key controls and compliance activities to be performed by component management in order to determine the Department's compliance with A-123. The OCFO described that they plan to incorporate Attachment R into Track Two of the ICOFR Playbook, which will aid DHS components in testing IT General Controls (ITGC) as part of the ICOFR Self Assessment process.

The OCFO and OCIO have made progress in creating a strategy for resolving material weaknesses and building management assurances through the CAP process and performing compliance testing. However, there is currently limited correlation between the POA&M process, the CAP process, Attachment R, and the strategies detailed in the ICOFR Playbook. The CAP process is an established process which has been used by the Department to track and resolve material weakness conditions, whereas the POA&M process has only recently been used in earnest by DHS as a tool to monitor IT weaknesses and corrective actions.

Currently, the OCFO, OCIO, and component OCFOs and OCIOs need to better understand and integrate the role of IT general and application controls in the ICOFR process. A gap exists between the OCFO and OCIO in managing IT weaknesses. IT audit findings are primarily addressed by the component OCIOs with little or no involvement from the OCFO, although such weaknesses also impact the financial processes. Ideally, the component OCFOs and OCIOs should collaborate more fully in order to address IT weaknesses and determine the impact to the financial processes in support of the ICOFR process. We recognize that some IT weaknesses are technical in nature and only require corrective action from the OCIO. However, the majority of IT weaknesses involve both the OCFO and OCIO and will require a collaborative effort to remediate the weakness. If both the OCFO and OCIO are not involved in addressing IT weaknesses, it is unlikely that IT general and application controls weaknesses will be resolved in a timely manner, as the correct personnel and necessary funding may not be dedicated to the remediation activities. However, if the OCIO and OCFO can in unison work to address IT weaknesses, management should be able to place increased reliance on the IT general controls environment and financial application controls and should be able to improve the overall DHS ICOFR process.

Recommendations

We recommend that the DHS OCFO and OCIO work together to develop detailed standard operating procedures (SOP) for identifying and addressing each IT weakness and/or audit finding. These SOPs should include a recommended approach to address IT findings in a collaborative effort from both the CIO and CFO. This collaborative management approach should include procedures to:

1) Delineate responsibility and ownership over remediation efforts in order to begin planning corrective action steps;

2) Identify the necessary resources and funding sources for the planned corrective actions; and

3) Perform corrective action jointly, where applicable.

Management Comments and OIG Evaluation

We obtained written comments on a draft of this report from the DHS OCIO and the components. Generally, the DHS OCIO and the components agreed with all of the report's findings and recommendations. We have incorporated the comments below and included a copy of the comments in the entirety at Appendix D.

The components will conduct root cause analysis on the FY08 financial system security findings before entering system POA&Ms and the OCIO will update the POA&M process guide section 3.1 and the POA&M creation checklist to clarify each NFR recommendation requiring a separate POA&M be identified.

The components will ensure that validation of each new POA&M, as well as for every change in POA&M status and the OCIO will update the DHS SSP Attachment H POA&M Process Guide to clarify and expand the component's responsibilities to performing testing and closure validations.

The OCIO will continue to implement the DHS 4300 A Sensitive System Policy (SSP) that identifies and addresses each IT weakness remediation effort and include an approach to address the findings in a collaborative effort from both the component CIO and CFO.

OIG Response

We agree with the steps that OCIO and components are taking to satisfy these recommendations.

Appendices

APPENDIX A

Background

Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control,* states "Federal agencies are subject to numerous legislative and regulatory requirements that promote and support effective internal control. Effective internal control is a key factor in achieving agency missions and program results through improved accountability. Identifying internal control weaknesses and taking related corrective actions are critically important to creating and maintaining a strong internal control infrastructure that supports the achievement of agency objectives."

OMB Circular A-123 builds upon the internal control framework within the *Standards for Internal Control in the Federal Government* (Green Book), issued by the Government Accountability Office (GAO), which defines internal control as "an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations."

OMB Memorandum 04-25, *Fiscal Year (FY) 2004 Reporting Instructions for the Federal Information Security Management Act,* "requires agencies to prepare Plans of Action and Milestones (POA&Ms) for all programs and systems where an Information Technology (IT) security weakness has been found. The guidance directs Chief Information Officers (CIO) and agency program officials to develop, implement, and manage POA&Ms for all programs and systems they operate and control (e.g., for program officials this includes all systems that support their operations and assets). Additionally, program officials shall regularly (at least quarterly and at the direction of the CIO) update the agency CIO on their progress to enable the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB."

Ten material weaknesses associated with internal controls were reported in DHS' Independent Auditor's Report included in the FY 2006 *Performance and Accountability Report.* One of these ten material weaknesses concerns financial systems security. In order to address the issues related to the financial systems security material weakness, the DHS Office of the Chief Information Officer (OCIO) and components track IT weaknesses and corrective action in POA&Ms. DHS components use an automated tool, Trusted Agent FISMA (TAF) to prepare POA&Ms and support the POA&M process.

DHS has also undertaken an initiative to develop and implement formal Corrective Action Plans (CAP) to resolve the remaining nine material weaknesses. Under this initiative, the Department has issued guidance and has also deployed a web-based software application, Electronic Program Management Office (ePMO), to manage the collection and reporting of CAP information for the Department and its components. Under this initiative, the Department's intent is to develop effective CAPs and position itself to move forward in its objective of obtaining an unqualified audit opinion on its consolidated financial statements, as well as on its internal controls over financial reporting.

APPENDIX B

Objectives, Scope, Methodology, and Criteria

Objectives

This performance audit is the first in a series of four performance audits the Office of Inspector General (OIG) engaged us to perform in regards to the DHS CAP and IT POA&M processes used to address material weaknesses cited in the Independent Auditors' Report included in the Department's FY 2006 *Performance and Accountability Report.* This portion of the performance audit has four sub-objectives:

1) Evaluate and report on the status of the Department's overall plan to develop well-written POA&M's, to include milestones and specific, actionable steps to correct DHS' material weakness in internal control related to financial IT systems.
2) Evaluate adherence by the components to milestones and continued steady progress.
3) Evaluate POA&M milestones and actionable steps to determine if they are consistent with DHS' planned financial system consolidation.
4) Evaluate and report upon the linkage that the IT POA&Ms have with OMB Circular A-123 guidance issued by the DHS Chief Financial Officer (CFO).

Scope

We evaluated the IT POA&Ms which relate to the financial systems security material weakness at four DHS components:

- United States Coast Guard;
- Transportation Security Administration;
- Federal Emergency Management Agency; and
- Immigration and Customs Enforcement.

Additionally, the scope included an assessment of the DHS OCIO's role within the POA&M process. Finally, our scope included a review of the IT POA&Ms and the linkage with the DHS planned financial system consolidation, as well as the Internal Controls Over Financial Reporting (ICOFR) Playbook.

We conducted our testing at DHS Headquarters and component locations through inquiry of agency management and personnel, observation, and inspection of relevant documentation. We performed our testing during the period of November 15 through December 12, 2007.

Methodology

We conducted our testing through inquiry of DHS management and personnel, and inspection of relevant documentation. Some of the inquiries we conducted of DHS management and personnel, included, but were not limited to the POA&M process, POA&M roles and responsibilities, the planned DHS financial system consolidation effort, the ICOFR Playbook, and implementation of OMB Circular A-123 requirements. Some examples of inspection of documentation included, but were not limited to: component 4th Quarter FY 2007 POA&M reports, DHS guidance and training materials for the POA&M process, the ICOFR Playbook, and DHS Corrective Action Plan guide.

The audit was conducted in accordance with *Generally Accepted Government Auditing Standards* (GAGAS), issued by the Comptroller General of the United States, and included such tests as we considered necessary to satisfy the objectives of the audit.

Criteria

Guidance for our performance audit included DHS information security policies, such as the DHS 4300A, *Sensitive Systems Handbook*, Attachment H, *POA&M Process Guide,* as well as OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, and OMB Memorandum 02-09, *Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones.*

APPENDIX C

Acronyms and Abbreviations

A-123	OMB Circular A-123
CAP	Corrective Action Plan
CFO	Chief Financial Officer
CIO	Chief Information Officer
DHS	Department of Homeland Security
ePMO	Electronic Program Management Office
FEMA	Federal Emergency Management Agency
FFMIA	Federal Financial Management Improvement Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
ICE	Immigration and Customs Enforcement
ICOFR	Internal Controls Over Financial Reporting
ISSM	Information System Security Manager
IT	Information Technology
ITGC	Information Technology General Controls
IV&V	Independent Verification and Validation
KPMG	KPMG LLP
NFR	Notice of Finding and Recommendation
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action & Milestones
RMTO	Resource Management Transformation Office
SOP	Standard Operating Procedures
TAF	Trusted Agent FISMA
TSA	Transportation Security Administration
USCG	United States Coast Guard
USSGL	United States Standard General Ledger

Appendix D

Management Comments

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

MAR 05 2008

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technology

Wayne Bavry

FROM: for Robert West
Chief Information Security Officer

SUBJECT: *Review of DHS Component Plans of Action and Milestones for Financial System Security (Draft),* Dated February 11, 2008.

Thank you for providing a copy of your draft letter report describing the implementation status of the Department of Homeland Security (DHS) Plan of Action and Milestones (POA&M) process supporting financial systems security. The Office of Information Security (OIS) generally concurs with the recommendations. Attachment A to this letter provides additional information on current procedures and projected remediation activities. Once the final report is released, POA&Ms will be opened by OIS and the DHS Component ISSMs will be directed to support improved FY08 POA&M processes for financial systems.

My office and the OCFO continue to address joint training and assessment activities to support both remediation and compliance requirements. I am requesting additional funding starting in FY10 in order to increase OCIO support for financial system requirements based on OMB A-123 requirements.

Should you have any questions or need further clarification please contact Wayne Bavry at the OCIO OIS, 202-282-9506, or Michael Wetklow at the OCFO Internal Control Program Management Office, 202-447-5196.

cc: Charles Armstrong, DHS CIO, Acting
David Norquist, DHS CFO
Dessadra Lomax, DHS CIO Audit Liaison Office
Penny McCormack, DHS GAO/OIG Liaison Office
Elisa R. Cruz, FEMA ISSM
Gil Vega, ICE ISSM
Jill Vaughn, TSA ISSM
Michael Massino, USCG ISSM

Attachments:

A. OIS Comments on OIG-08-Draft, *Review of DHS Component IT Plans of Action and Milestones for Financial System Security,* Dated February 11, 2008.
B. DHS 4300A, *Sensitive Systems Handbook,* Attachment H, *POA&M Process Guide,* Version 6.0, dated January 1, 2008.
C. OCIO Root Cause Analysis Training Material – Preliminary, March 2008

Attachment A: OIS Comments *Review of DHS Component Plans of Action and Milestones for Financial System Security,* Dated February 11, 2008

Finding and OIG Recommendation 1:

We recommend that FEMA, ICE, TSA, and USCG:

1) *Conduct a formal root cause analysis for IT weaknesses in order to determine the appropriate corrective actions.*
   a) *identify and walk through the process associated with the weakness*
   b) *Perform an analysis to determine gaps within the process*
   c) *Find the root cause contributing to the gaps within the process*
   d) *Develop and implement identified solutions; and*
   e) *Observe the implementation of the solution to ensure effectiveness*

2) *Review existing POA&M weaknesses and milestones to confirm that the root cause is being addressed.*

3) *Require the component Information System Security Manager (ISSM) to verify that the component is creating unique POA&M milestones to address the root cause of identified weaknesses, rather than using the NFR recommendations as milestones.*

4) *Require that the component ISSM ensure that POA&M milestones include reasonably scheduled completion dates.*

Additionally, we recommend that the OCIO:

1) *Update DHS 4300A, Attachment H, to include the requirement for quarterly milestone completion dates, as well as to prohibit components from using NFR recommendations as milestones, unless the root cause analysis is in agreement with the NFR recommendations.*

2) *Enhance root cause analysis guidance and training provided to component personnel.*

OCIO Consolidated Component Response:

1) **Concur.** All Components identified on the FY08 CFO designated financial systems will be directed by the DHS CISO to conduct root cause analysis on FY08 financial system security findings before entering system POA&Ms.

2) **Concur.** Many Components are expected to have closed FY07 POA&Ms prior to receiving the recommendations in the final report, therefore any re-issued recommendations must further address root cause analysis in their FY08 remediation plans.

3) **Concur.** Currently the FY08 Components scorecards require each NFR recommendation be addressed with a POA&M. Component POA&M scores will be reduced if each NFR's recommendation is missing a POA&M. ISSMs are currently required to validate each POA&M provides unique milestones. In FY08 ISSMs will be directed to ensure root cause analysis has been completed and milestones are unique.

4) **Concur.** Currently the FY08 Component scorecards track compliance against a reasonableness criteria for both schedule and resources, as identified in the *DHS 4300A, Attachment H,* Appendix F. Component scorecards also track ISSM validation of these factors.

No Component POA&Ms are required.

Attachment A: OIS Comments *Review of DHS Component Plans of Action and Milestones for Financial System Security,* Dated February 11, 2008

OCIO Response:

1) **Concur.** Currently DHS 4300A, Sensitive Systems Handbook, Attachment H, POA&M Process Guide, Version 6.0, dated January 1, 2008 (Attachment B), Section 3.4 recommends;

   Milestones should be developed not only to address the specific weakness that has been identified but also the underlying cause of that weakness to ensure the weakness does not recur. Additionally, if the weakness will take several months to resolve, multiple milestones should be used to show interim steps which can be used to track progress. It is recommended that at least one milestone be included for approximately every 3-4 months of schedule.

   The POA&M Process Guide Section 3.1 and POA&M Creation Checklist will be updated to clarify each NFR recommendation requires a separate POA&M be identified, to further preclude Components from opening a single POA&M for each NFR supporting multiple recommendations.

An OIS POA&M will be opened to complete this recommended activity.

POC: Wayne Bavry

2) **Concur.** OIS provided root cause analysis training as part of the OCIO's Workshops on Financial System Security held in January and August 2007. To date in FY08, more than 200 people in 14 Components have received POA&M related training.

   a. OIG/KPMG and the OCFO will be requested to provide feedback to the OIS on NFR Root Cause analysis training material as identified in Attachment C.

   b. The POA&M Process Guide will add an Appendix to provide a more formal methodology for addressing root cause analysis, including worksheets to support the analysis activity.

   c. The POA&M Process Guide will also be updated to specify additional ISSM validation requirements including the completion of a root cause analysis.

   d. The joint CFO-CIO FY08 Component ITGC assessment process will include training on a more formal methodology for performing root cause analysis.

   e. The FY08 POA&M training will be updated to include a more formal methodology for performing root cause analysis.

   f. The annual DHS Security Conference will, as part of the POA&M training session, include a more formal methodology for performing root cause analysis.

An OIS POA&M will be opened to complete these six activities.

POC: Wayne Bavry

Attachment A: OIS Comments *Review of DHS Component Plans of Action and Milestones for Financial System Security*, Dated February 11, 2008

Finding and OIG Recommendation 2:

We recommend that FEMA, TSA, and USCG create and implement an internal independent verification and validation (IV&V) process to verify and document the status of POA&M weaknesses. This process should include approvals for closure by the component ISSM and require the upload of artifacts into Trusted Agent FISMA (TAF) to support the closure of the NFRs.

Additionally, we recommend the OCIO to update DHS 4300A, Attachment H to require that components include testing and closure validation as a milestone for each POA&M weakness in order to verify that weaknesses are properly closed.

OCIO Consolidated Component Response:

Concur. The DHS *FY08 Performance Plan* currently requires ISSM validation for each new POA&M, as well as for every change in POA&M status (i.e. delayed, cancelled or completed). This is considered an internal independent verification and validation process on the POA&M weakness status.

The DHS SSP Attachment H *POA&M Process Guide* Section 3.4 currently recommends Components include testing and documentation as a milestone for each POA&M. This recommendation is also included in POA&M training.

No Component POA&Ms are required.

OCIO Response:

Concur. The DHS SSP Attachment H *POA&M Process Guide* will be updated further to clarify and expand the Component's responsibilities to performing testing and closure validation as a milestone for each POA&M in order to verify that audit identified weaknesses are properly closed.

An OIS POA&M will be opened to complete this recommended activity.

POC: Wayne Bavry

Attachment A: OIS Comments *Review of DHS Component Plans of Action and Milestones for Financial System Security,* Dated February 11, 2008

Finding and OIG Recommendation 3:

We recommend that the DHS OCFO and OCIO work together to jointly develop detailed standard operating procedures (SOP) for identifying and addressing each IT weakness and/or audit finding. These SOPs should include a recommended approach to address those findings in a collaborative effort from both the component CIO and CFO. This collaborative management approach should include a process to:

1) Delineate responsibility and ownership over remediation efforts;
2) Identify the necessary resources and funding sources; and
3) Plan to perform corrective action jointly, where appropriate.

OCIO Response:

1) **Concur.** Currently DHS 4300A *Sensitive System Policy (SSP)* Section 2.15 delineates the System Owner's responsibilities for remediation efforts:

   •Ensure that system POA&Ms are prepared and maintained and that point of contact and resources are identified
   • Prioritize security weaknesses for mitigation based on material weaknesses, external audits and program assessments

   SSP Section 3.9 also delineates *the Component CIO shall serve as DAA anytime the system owner or an appropriate program official cannot be named.*

   SSP Attachment H, *POA&M Process Guide,* Section 2.2 delineates responsibility and ownership over IT remediation efforts. Section 3.2 also provides guidance regarding inclusion of all appropriate people in formulating and implementing a remediation plan.

   No OIS POA&M is required.

2) **Concur.** Currently DHS 4300A SSP Section 3.2.b states System owners or DAAs shall ensure that IT security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.

   DHS 4300A, SSP Attachment H, *POA&M Process Guide,* Section 3.4 provides guidance on determining required resources.

   No OIS POA&M is required.

3) **Concur.** Currently DHS 4300A SSP Section 2.18.1 indicates the DHS CFO is responsible for remediating "automated application control deficiencies related to financial application policies and procedures at the Department level." Section 2.18.3 indicates the Component CFO is responsible for remediating "automated application controls deficiencies at the Component level."

   In FY06 and FY07 Component's Financial System Remediation meetings were held with the DHS CIO and DHS CFO in order to further address any joint responsibilities. An annual meeting with senior management is also projected for the FY08 audit.

   No OIS POA&M is required.

Appendix E

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
DHS Chief Information Officer
DHS Chief Financial Officer
DHS Chief Information Security Officer
FEMA Chief Information Officer
TSA Chief Information Officer
US Coast Guard Chief Information Officer
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees as Appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- **Call our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**
  DHS Office of Inspector General/MAIL STOP 2600, Attention:
  Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.